WILLIAM BROOKES SCHOOL

The 3-18 Education Trust

E-Safety Policy

Member of Staff Responsible	CEO (statement of intent for trust), Headteacher for procedure and implementation of e-safety at school.
Relevant guidance/advice/legal reference	KCSiE (2021)
Adopted by	Individual schools and trust office
Date of Policy	January 2022
Review Cycle	3 years
Date of Next Review	January 2025

This policy is in two sections.

Section 1: this covers the trust-based intention for e safety and recognises the link with the Prevent duty, use of mobile phones and general cyber security.

Section 2: the school's and trust's implementation of the policy.

Section 1 (Trust)

Statement of Intent (from the Trust)

This policy is not a statutory requirement, but its existence recognises the significance of students and staff remaining safe whilst accessing resources online.

The 3-18 Education Trust has the highest regard for E-safety in its schools in order to promote safe and responsible use of technology. We are committed to using new technology to enhance the curriculum and educational opportunities whilst equipping our children and young people with the knowledge and understanding to stay safe and vigilant when online, both in school and outside.

E-safety involves the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media (e.g. text messages, email, gaming devices).

E-safety is not just about technology, it is also about people and their actions.

Technology provides unprecedented access to new educational opportunities through online collaboration, learning and communication. At the same time, it can provide the potential for staff and students to access material they should not access or it may lead to staff and students being treated by others inappropriately.

E-safety is part of the wider duty of care of all those who work in schools: equipping children and young people to stay safe online, both in school and outside and is integral to a school's ICT curriculum. It may also be embedded in Personal Social and Health Education (PSHE) and Relationships, Sex and Health Education and include how staff and students should report incidents

Advice and resources on internet safety are available at: https://www.saferinternet.org.uk/
In association with the relevant Acceptable Use Policy Agreement (AUP), this policy forms part of the school's commitment to educate and protect all users when accessing digital technologies, both within and outside school. It should be read in conjunction with other relevant policies, such as the Child Protection and Behaviour policies.

The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable to regulate the behaviour of students when they are off the school site and (the Act) empowers members of staff to impose sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school but which are linked to membership of the school.

Schools will, where it becomes known, inform parents/carers of any such incidents of inappropriate online behaviour that takes place out of school.

The 2011 Education Act increased these powers with regard to the searching for electronic devices and the examination of any files or data (even where deleted), on such devices.

The Prevent Duty (See Preventing Radicalisation and Extremism Policy)

As organisations seek to influence young people through the use of social media and the internet, schools and childcare providers need to be aware of the increased risk of online radicalisation and the risks posed by the online activity of extremist and terrorist groups.

The Prevent duty is the duty under the Counter-Terrorism and Security Act 2015 on specified authorities (schools and childcare providers), in the exercise of their functions, to have due regard for the need to prevent people from being drawn into terrorism. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

The Prevent duty means that all staff have a duty to be vigilant, and where necessary, will report concerns about internet use that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

https://www.educateagainsthate.com/

The use of devices in school, which are not owned by school

Mobile phones: If a student wishes to bring these into school, they must be switched off and put away (kept out of sight). The trust recognises the value that a mobile phone can have at the start and finish of the school day, but also the significant distraction and potential harm that the use of a mobile phone can bring when used in school.

Students found to be in breach of this requirement will have their device confiscated. These can be collected at the end of the day. If a member of staff suspects that a mobile phone has been misused within the school, then it should be confiscated and the matter dealt with in line with normal school procedure (see below).

Cyber bullying

All forms of bullying (including cyberbullying) should be handled as a community issue for the whole school. Every school has measures in place to prevent all forms of bullying. These measures should be part of the school's behaviour policy which are communicated to all pupils, school staff, governors and parents.

Cyber bullying is defined as '*the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them*.'

Cyber bullying against staff

The DfE state that '*all employers, including employers of school staff in all settings, have statutory and common law duties to look after the physical and mental health of their employees. This includes seeking to protect staff from cyberbullying by pupils, parents and other members of staff, and supporting them if it happens*'.

Cyberbullying: Advice for headteachers and school staff is non-statutory advice from the Department for Education for headteachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Section 2: School-based implementation and policy

Individual schools are responsible for their E-Safety procedures and are given freedom to manage their provision. This is due to their different contexts with respect to key stages. Day to day responsibility for educating pupils in E-safety settings lies with the headteachers and other staff with responsibility for the IT provision in schools.

The E-safety policy applies to all members of the school community, including staff, governors, pupils, volunteers, parents, carers, and visitors. This includes anyone who uses and/or has access to, personal devices and technologies whilst on school site and those who have access to, and are users of, school devices and technologies, both in and outside of the school.

Purpose

The purpose of this statement is to outline how the school will deliver safe and responsible use of ICT throughout school and give clear guidelines (Acceptable Use Agreements) to staff, pupils and volunteers.

Roles and responsibilities

Head	□ Has overall responsibility for E-safety provision. □ Has overall responsibility for data and data security □ Ensures that the school uses an appropriate filtered Internet Service □ Ensures that staff receive appropriate training to enable them to carry out their E-safety roles □ Can direct the whole school community including staff, students and governors to information, policies and practice about E-safety. □ Is aware of the procedures to be followed in the event of a serious E-safety incident. □ Ensures that there is a system in place to monitor and support staff who carry out internal E-safety procedures and reviews (e.g. Network Manager). □ Oversees the administration of the staff Acceptable Use Policy Agreements and takes appropriate action where staff are found to be in breach.
Designated Safeguarding Lead	□ Takes day to day responsibility for E-safety issues and assumes a leading role in establishing and reviewing the school E-safety policies and supporting documents. □ Ensures that the school is compliant with all statutory requirements in relation to the handling and storage of information. □ Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the *Data Protection Act* 1998. □ Promotes an awareness of and commitment to E-safety throughout the school community. □ Ensures that E-safety is embedded across the curriculum. □ Is the main point of contact for students, staff, volunteers and parents who have E-safety concerns.

	Ensures that staff and students are regularly updated on E-safety issues and legislation, and are aware of the potential for serious child protection issues that arise from (for example): - sharing of personal data - access to illegal/inappropriate materials - inappropriate on-line contact with adults/strangers - cyber-bullying Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident. Ensures that an E-safety incident log is kept up to date. Liaises with school IT technical staff where necessary and/or appropriate. Facilitates training and provides advice and guidance to all staff. Communicates regularly with SLT to discuss current issues, review incident logs and filtering.
Head of ICT	Oversees the delivery of the E-safety element of the Computing curriculum. ⍰ Oversees the delivery of the E-safety element of the Computing curriculum. ⍰ Communicates regularly with the E-safety coordinator.
All Staff	Read, understand and help promote the school’s E-safety policies and guidance. Are aware of E-safety issues relating to the use of any digital technology, monitor their use, and implement school policies with regard to devices. Report any suspected misuse or problem to the E-safety coordinator. Maintain an awareness of current E-safety issues and guidance, e. g. through training and CPD. Model safe, responsible and professional behaviours in their own use of technology. Ensure that any digital communications with students are on a professional level and through school-based systems ONLY. Ensure that no communication with students, parents or carers is entered into through personal devices or social media. Ensure that all data about students and families is handled and stored in line with the principles outlined in the Staff AUP.
Teaching Staff	Embed E-safety issues in all aspects of the curriculum and other school activities. • Supervise and guide students carefully when engaged in learning activities involving online technology (including extracurricular and extended school activities, where relevant). • Ensure that students are fully aware of how to research safely online and of potential legal issues relating to electronic content such as copyright laws.
Students	•Are responsible for using the school digital technology systems in accordance with the Student AUP Agreement. •Have a good understanding of research skills, the need to

	avoid plagiarism and to uphold copyright regulations. •Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. •Understand policies on the use of mobile devices and digital cameras, the taking and use of images and cyber-bullying. •Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions, in and out of school, if related to their membership of the school.
Parents/Carers	Parents and carers are encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: • digital and video images taken at school events. • access to parents' sections of the website/ Learning Platform and on-line student/student records. • their children's personal devices in the school.
External groups	Any external individual/organisation must sign an Acceptable Use Policy prior to using any equipment or the Internet within the school.

Acceptable use policies (and breaches) – Staff, students
Use of devices (passwords, data storage (data protection) emails, phones, photographs)

1. Using non-School Equipment – 'Bring Your Own Device/Bring Your Own Technology' (BYOD/BYOT)

Under some circumstances, staff, governors and students are able to use their own devices in school and connect to the school network. This is normally referred to as 'Bring Your Own Device'/'Bring Your Own Technology' (BYOD/BYOT). Regardless of the ownership of the device, the rules and expectations of online behaviour are as set out in the relevant AUP.

2. Security and passwords

Passwords should be changed regularly and must not be shared. The school system will inform users when the password is to be changed. Staff must always 'lock' a device (e.g. a classroom PC) if they are going to leave it unattended. NB. The picture 'mute' or picture 'freeze' option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked'. All users should be aware that the ICT system is filtered and monitored.

3. Data storage

All staff and students have access to One Drive. One Drive can be used to store and access files both in school and at home. Other storage devices should not be used in school. Only authorised and encrypted USB devices are to be used in school after gaining permission from the Network Manager.

4. Mobile phones, cameras and other devices

The school's policy relating to the use of devices such as mobile phones, is set out in the relevant AUP.
Student devices such as mobile phones, should be switched off whilst on the school premises and kept out of sight. Students found to be in breach of this requirement will have their device confiscated and sent to the reception marked with the student's name and tutor group.
Confiscated phones can be collected by students or parents/carers for repeat offenders at the end of the school day.
If a member of staff suspects that a mobile phone has been misused within the school, then it should be confiscated, and the matter dealt with in line with normal school procedure and/or the Behaviour policy. All staff are required to adhere to the AUP which sets out the expected use of mobile phones whilst on duty.

Photos taken by the school are subject to the Data Protection Act.

Process of reporting

The school takes the reports of incidents and concerns extremely seriously. Any subsequent action or remedy to be taken following the investigation of an incident or concern, will depend on its nature, situational and circumstantial factors.

All incidents that come to the attention of school staff should be notified to the DSL via CPOMS, the school reporting mechanism as set out in the school's Child Protection Policy, or, where applicable, via the Whistleblowing Policy.
Any incident that raises child protection or wider safeguarding questions must also be communicated to the Designated Safeguarding Lead(s) immediately.
Incidents that are of a concern under the Prevent duty should be referred to the Designated Safeguarding Lead, immediately and recorded on CPOMS. Incidents which are not child protection issues but may require SLT or pastoral intervention (e.g. cyberbullying) should be reported to Heads of House and SLT, immediately.

Training

Staff

All staff have E-safety training included as part of their safeguarding induction to the school and receive training in safeguarding students. E-safety is included as part of this.

Students

Acceptable Use Policy Agreement is given to all students during induction and then reviewed by all students at the start of September. The aim is to make the policy familiar and accessible to all students at all times. Students are made aware that network and Internet use is monitored.

Appendix A – AUP for Staff & Volunteers

AUP for Staff & Volunteers

I understand that I have personal and legal responsibilities, including treating others with dignity and respect, acting honestly, using public funds and school equipment appropriately, adhering to health and safety guidelines and safeguarding pupils at all times.

I understand that I must use school devices and systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of systems and other users.

I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to benefit from the use and application of appropriate digital technology.

I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with children and young people.

Professional and personal safety:

□ I understand that the school has in place a filtering system and will monitor my access to digital technology and communications systems whilst using school devices, and/or access to the school network via personal devices, where such access has been granted.

□ I understand that the rules set out in this agreement also apply to use of school devices and digital technologies out of school, and to the transfer of personal data (digital or paper based) out of school.

□ I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use in line with the general principles of this agreement and the expectations of professional behaviour set out in the Staff Code of Conduct.

□ I will not disclose my password to anyone else, nor will I try to use any other person’s username and password. I understand that I should keep passwords safe and not share them with anyone.

□ I will immediately report any incidence of access to illegal, inappropriate or harmful material, deliberate or accidental, by myself or others, to the DSL.

□ I will not install or attempt to install programmes of any type on a device, nor will I try to alter computer settings, unless this is permitted by the Network Manager.

□ I will not deliberately disable or cause any damage to school equipment, or the equipment belonging to others.

□ I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy

□ I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when required by law, or by school policy, to disclose such information to an appropriate authority.

□ I will immediately report any damage or faults involving devices or software, however this may have happened.

□ I will ensure that I have permission to use the original work of others in my own work.

□ Where work is protected by copyright, I will not download or distribute copies (including music and videos).

□ I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

□ I will log out of a device when I have finished using it.

□ I will lock my computer when I leave it unattended.

Electronic communications and use of social media:

□ I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

□ I will use social networking sites responsibly, taking care to ensure that appropriate privacy settings are in place, and ensure that neither my personal nor professional reputation, nor the school's reputation, is compromised by inappropriate postings, to include past postings.

□ I will never send or accept a 'friend request' made through social media from a student at school. I understand that such requests should be raised formally as an incident.

□ I will not, under any circumstances, make reference to any staff member, student, parent or school activity/event via personal social media or other communication technologies.

□ I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner. At no time will I use or share a personal email address, phone number or social networking site for such communication purposes.

□ I will notify the Headteacher of any current or future, direct or incidental contact with students, parents or carers, for example where parents or carers are part of the same social group.

□ I will not engage in any online activity, at, or outside school, that may compromise my professional responsibilities. This includes making offensive, aggressive or defamatory comments, disclosing confidential or business-sensitive information, or information or images that could compromise the security of the school.

□ I will not use the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material, online or in print.

□ I will not post any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school.

Use of school and personal mobile devices and technologies

□ When I use my own mobile device (e.g. laptop / tablet / mobile phone / USB device) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

□ I will keep my personal phone numbers private and not use my own mobile phone, or other device, to contact students or parents in a professional capacity.

□ I will keep my mobile phone secure whilst on school premises. It will be switched off whilst I am on duty unless there are good reasons that have been approved with a member of the senior leadership team, and then that is discreet and appropriate, e.g. not in the presence of students.

□ I will keep mobile devices switched off and left in a safe place during lesson times. I understand that the school cannot take responsibility for personal items that are lost or stolen.

□ I will report any text or images sent to me by colleagues or students which could be viewed as inappropriate. I will not use a personal device to photograph a student(s), except with the written permission of the Headteacher.

□ I will not use personal email addresses on the school ICT systems.

□ I will not open any hyperlinks in emails or any attachments to emails if I have any concerns about the validity of the email or its source is neither known nor trusted.

□ I will, when I take and/or publish images of others, do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use any personal devices to record these images, unless I have written permission from the Headteacher. Where these images are approved by the school to be published (e.g. on the school website) it will not be possible to identify by name, or any other personal information, those who are featured.

□ I will not attempt to upload, download or access any material which is illegal (for example; images of child sexual abuse, criminally racist material, adult pornography), inappropriate or may cause harm or distress to others.

□ I will not attempt to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

□ I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

Conduct and actions in and out of the school:

□ I understand that this Acceptable Use Policy applies not only to my work and use of school devices and digital technology in school, but also applies to my use of school systems and equipment off the premises. This Acceptable Use Policy also applies to my use of personal devices on the premises or in situations related to my employment by the school.

□ I understand that should I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action in line with the school's agreed Disciplinary Procedure. In the event of any indication of illegal activity, I understand the matter may be referred to the appropriate agencies.

I have read and understood the above, and agree to use school devices and access digital technology systems (both in and out of school), as well as my own devices (in school and when carrying out communications related to the school), within this agreement.

I understand that in the event of any query or concern about this Agreement, I should contact the school DSL.

Staff/Volunteer Name:	
Signed:	
Date:	

Appendix B – Students AUP

Student Acceptable Use Policy

The policy aims to ensure that any communications technology is used without creating unnecessary risk to others.

I agree that I will:

□ respect the school network security

□ set strong passwords which I will not share

□ only use, move and share personal data securely

□ not use my own mobile phone, or any other device, in school, unless I am given permission by a member of staff

□ only visit sites which are appropriate

□ always follow the terms and conditions when using a website

□ respect copyright and the intellectual property rights of others

□ only create and share content that is legal

□ not access social networking sites or apps whilst at school

□ only use approved email accounts (@williambrookes.com) to communicate with staff

□ only use appropriate content which I have permission to use

□ only communicate online with trusted users

□ never meet an online friend without taking a responsible adult that I know with me

□ make sure all messages/posts I send are respectful

□ not respond to or forward any inappropriate message or content

□ be cautious when sharing personal contact information

□ only communicate electronically with people I know or have been approved by my school

□ report unsuitable content or activities to a member of staff

I know that anything I share online at school via the school network may be monitored by the school.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I am aware of the CEOP Report button and know when to use it. CEOP REPORT ceop.police.uk

I agree that I will not:

□ act in a way that might breach the school Behaviour policy

□ attempt to breach the security on the school network

□ forward chain letters

□ breach copyright law

□ do anything which exposes others to harm or danger

□ produce/distribute any information which may be offensive to others

□ visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

□ inappropriate images
□ promoting discrimination of any kind
□ promoting violence or bullying
□ promoting racial or religious hatred
□ promoting illegal acts

I accept that my use of both school and personal devices may be monitored and reported on.

Student Name:		Student Signature:	
Tutor Group:		Date:	

Appendix C – Digital Devices

Guidelines for Use

1.Use of personal devices during the school day is at the discretion of teachers and staff. Students must use devices as directed by their teacher.
2.The primary purpose of the use of personal devices at school is educational. Using the device for personal reasons, e.g. playing games should only take place during your social time.
3.The use of a personal device is not to be a distraction in any way to teachers or Students.
4.The use of personal devices falls under William Brookes School's Acceptable Use Policy, found on the school portal.
5.Students shall not use personal devices outside of their classroom unless otherwise directed by their teacher e.g. on school visits or activities.
6.Students shall make no attempts to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.
7.Students shall not take pictures or video of Students or staff without their permission. Pictures or videos should not be distributed (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).
8.Your school email account must be set up on the device.
9.Android and Windows devices should have antivirus and spyware software installed.
10.Mobile phones should not be used for communication, e.g. texting, making calls, using social media or messaging during the school day.

Consequences for Misuse/Disruption (one or more may apply):

1.Device removed by teacher until the end of the day.
2.Access to the wireless network will be removed.
3.Device taken away for two nights.
4.Device taken away and kept until parent picks it up.
5.Student is not allowed to use personal devices at school.

Serious misuse of Internet capable devices is regarded as a serious offence within the School's Behaviour Management Policy and will be dealt with in accordance with this policy.

School Liability Statement

Students bring their devices to use at William Brookes School at their own risk. Students are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices. William Brookes School is in no way responsible for:

1. Personal devices that are broken while at school or during school-sponsored activities
2. Personal devices that are lost or stolen at school or during school-sponsored activities
3. Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

I understand the guidelines for use and the consequences for

Name:		Tutor Group:	
Signed:		Date:	
Parent/Guardian:		Signed:	
Device:		WIFI Address	
School Username:			

Appendix D - Legislation

Protection of Children Act 1978
Sexual Offences Act 2003
Public Order Act 1986
Obscene Publications Act 1959 and 1964
Human Rights Act 1988
The Education and Inspections Act
The Education and Inspections Act 2011
The Protection of Freedoms Act 2012
The School Information Regulations 2012
Serious Crime Act 2015